

Certified randomness in quantum physics

Antonio Acín^{1,2} and Lluís Masanes³

¹ICFO-Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

²ICREA-Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain

³Department of Physics & Astronomy, University College of London, London WC1E 6BT, United Kingdom

Abstract

The concept of randomness plays an important role in many disciplines. On one hand, the question of whether random processes exist is fundamental for our understanding of nature. On the other hand, randomness is a resource for cryptography, algorithms and simulations. Standard methods for generating randomness rely on assumptions on the devices that are difficult to meet in practice. However, quantum technologies allow for new methods for generating certified randomness. These methods are known as device-independent because do not rely on any modeling of the devices. Here we review the efforts and challenges to design device-independent randomness generators.

1 Introduction

Because of its importance, a significant scientific effort is devoted to understand when a given process generates “good” randomness. The process is represented by a device, or black box, producing bits, see Figure 1, which is in the user’s hands. What constitutes “good” randomness may depend on the application, but here we are interested in the strongest definition: N bits are *perfectly random* if they are unpredictable, not only to the user of the device, but to *any observer*. This definition is satisfactory both from a fundamental and applied perspective. On the one hand, while unpredictability by any observer may not be needed for some applications, such as Montecarlo simulations, from a fundamental perspective it is difficult to argue that a process is random if there could exist an observer able to predict its outcomes. On the other hand, by demanding that the results should look random to any observer, the generated randomness is guaranteed to be *private*: the user, by running the process in a secure location, has the guarantee that nobody knows the obtained results, which can later be safely used for cryptographic purposes.

According to this definition, *the generation of randomness from scratch is impossible*. This follows from the unfalsifiable hypothesis of the existence of a super-deterministic model in which everything, including all the history of our universe, was pre-determined in advance and known by the external observer. Thus, *any protocol for randomness generation must be based on some hypotheses or assumptions*. The appropriateness of the assumptions is often debatable and strongly depends on the application. From a fundamental point of view, a random number generator (RNG) is better than another if it is based on fewer or weaker assumptions. However, adding more assumptions may not compromise the use of the random bits for a specific application, while it may simplify the experimental implementation and/or increase the efficiency.

Here we adopt a physics-based approach to randomness generation: the random numbers should be unpredictable to any *physical* observer, that is, any observer whose actions are constrained by the laws of physics. In particular, and according to the current understanding of nature, the device generating the random numbers and the device held by the potential adversary should obey the laws of quantum physics. Within this theory, the joint state of the user U and the adversary E (which includes all the environment) describing N ideal random bits is

$$\rho_{UE} = \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \right)^{\otimes N} \otimes \rho_E . \quad (1)$$

This corresponds to N realizations of a perfect random bit, taking the value 0 and 1 with equal probability, which are totally uncorrelated with the state of the environment ρ_E . Given a device, we say that it generates *arbitrarily good randomness* if its output is undistinguishable from the ideal state (1), up to some controllable small error.

A fundamental issue when considering randomness generation is certification: how can the user certify that the numbers produced by his device are random? According to (1), the random bits should follow a uniform probability distribution and also be uncorrelated to the environment. Concerning the first point, the standard solution consists of running statistical tests [1] on sequences generated by the device. However, it is unclear what passing these tests means and, in fact, it is impossible to certify with finite computational power that a given sequence is random.

The certification of privacy is much subtler. The best way to illustrate this is by means of what we call the memory-stick attack. Imagine a situation in which the provider of the devices is the adversary and has access to a proper RNG. The provider uses it to generate a long sequence of good random numbers, stores them into a memory stick and sells it as a proper RNG to the user. The numbers generated by the user will pass any statistical test and look random. However, they are not properly random, as they can be perfectly predicted by the adversary.

The generation of good randomness is a notoriously difficult problem [2, 3]. There exist basically three types of approaches. Pseudo-random-number generators (PRNG) use an algorithm to process an initial random seed. They are fast, cheap and the properties of the generated sequences are good enough for some applications. However, the random character of the output and their privacy is based on assumptions on the computational power of the adversary. But this is not the criterion adopted here, as we demand unpredictability to any observer, independently of its computational power.

The second type of RNG are called True RNG (TRNG) and exploit physical processes that are hard to predict, such as meteorological phenomena or the mouse movements of a computer user. Finally, there are quantum RNG (QRNG), which exploit a quantum process believed to be fundamentally random. In what follows, we focus this discussion on QRNG, although many of the problems stated below also apply to TRNG.

The paradigmatic example of a QRNG is defined by the clicks observed after a single photon impinges a beam-splitter, see Figure 1. This is however an idealized theoretical situation that may be difficult, if not impossible, to perfectly meet in an experiment. Imperfections on the devices are unavoidable and may deteriorate the quality of the generated numbers in uncontrolled manners. It is also difficult to exclude memory effects, for instance at the detectors, which produce correlations among the generated bits. The privacy of the symbols follows from the fact that the single-photon state is assumed to be pure and therefore cannot be coupled to another system. Hence, there is plenty of assumptions on the working of the QRNG that are crucial to guarantee the perfect match between the ideal theoretical situation and the implementation, which is in turn necessary to guarantee the quality of the generated outputs.

The current certification method applied to QRNG consists of passing statistical tests. Apart from the problems already mentioned above, the use of these tests is even more doubtful for QRNG, as they can be satisfied by classical RNG too. So, the only guarantee the user has that the symbols have a quantum origin is trusting the provider. Finally, the user has no means to test the privacy of the symbols as he is unable to rule out the memory-stick attack. Trust is again the only solution. All this level of trust is unsatisfactory as (i) in many situations, especially for cryptographic applications, it is convenient to reduce the trust on the provider as much as possible, and (ii), even if the provider is trusted and has constructed the devices in the best possible way, uncontrolled drifts and changes on the devices are unavoidable and may deteriorate the quality of the generated randomness. There is a need for solutions that certify the quantumness, quality and privacy of QRNG without requiring any detailed modelling of the devices.

Device-independent quantum random-number generators (DIQRNG) offer a solution to the previous issues and provide protocols for generating certified randomness based only on general assumptions on the setup, such as, e.g., the validity of quantum physics. In particular, they do not require any assumption on the inner working of the devices, which can be seen as quantum black boxes processing classical information. The development of DIQRNG protocols is an active research field involving many concepts and methods, from information-theoretical studies to design stronger protocols based on weaker assumptions, to their experimental realization using current or near-future technology.

In what follows, we first show how randomness certification without assumptions on the inner working of the devices can be achieved by exploiting the quantum violation of Bell inequalities (Section 2). We then describe the state of the art in DIQRNG protocols (Section 3) and their experimental implementations (Section 4). As these implementations turn out to be challenging, we describe other approaches to certified randomness with milder experimental requirements in Section 5. Finally, in Section 6 we explain how, in addition to practical applications, protocols for certified randomness answer some fundamental questions in physics. We conclude with an outlook in Section 7.

2 Device-independent randomness generation

DIQRNG protocols make use of the correlations observed when measuring entangled particles that do not have a classical analogue, as certified by the violation of a Bell inequality [4]. The user now needs at least two separated devices for running a Bell test, see Figure 2. The devices receive classical inputs, x and y , and produce classical outputs a and b . After N_r rounds of collecting the data (x, y, a, b) , the user calculates the relative frequencies of the outcomes given the inputs $P(a, b|x, y)$, which can be estimated without making any assumption about the internal working of the devices. A Bell inequality is a linear function of these relative frequencies

$$\beta = \sum c_{abxy} P(a, b|x, y) \leq \beta_L , \quad (2)$$

characterized by some coefficients c_{abxy} . Here, β_L is the so-called local bound satisfied by classical theories à la Einstein-Podolsky-Rosen (EPR) [5]. The violation of the Bell inequality witnesses the presence of non-classical correlations between the two devices.

The idea behind DIQRNG is that if the user observes a Bell inequality violation, he has the guarantee that the unknown quantum state in the devices has certain entanglement and purity. The purity of the quantum state certifies that the two devices are not too correlated with the environment or the external observer. The entanglement certifies that the local state of one of the devices is mixed and, thus, a measurement on it generates random outcomes. Moreover,

the Bell certification of randomness is intrinsically *quantum*, as classical devices always satisfy a Bell inequality. Finally, it is *device-independent* as for its computation only the observed statistics $P(a, b|x, y)$ is needed.

Consider for instance the case in which the user tests the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [6] and observes its maximal quantum violation¹. Take the set of all possible correlations observed after applying local measurements $\Pi_{a|x}$ and $\Pi_{b|y}$ on the state describing the two quantum devices $|\Psi\rangle$,

$$P(a, b|x, y) = \langle \Psi | \Pi_{a|x} \otimes \Pi_{b|y} | \Psi \rangle. \quad (3)$$

Among all these quantum correlations, the only way of getting a maximal violation of the CHSH is when projective measurements are performed on a maximally entangled state of two qubits [7, 8, 9]

$$|\Psi\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (4)$$

As the state is pure, it cannot be correlated to the environment. The local measurements on half of it produce perfect random bits (1), which are certified by the observed Bell violation. This intuitive argument holds when the maximal quantum violation of the CHSH inequality is obtained. For noisy non-maximal violations, it is also possible to quantify the amount of randomness from the observed violation, see Figure 3.

While the previous discussion has exploited the properties of quantum correlations (3), it is even possible to design DIQRNG that do not rely on the validity of quantum theory but only on that of the no-signalling principle, that is, the impossibility of faster-than-light communication between devices. In fact, under the sole assumption of no-signalling, the violation of a Bell inequality guarantees the random character of the outputs [10, 11, 12, 13, 14, 15, 16].

All these nice features come at a price: the user should meet the conditions needed in (3). He has to make sure that:

- (C1): the inputs (x, y) have no correlations with the devices;
- (C2): there is no communication between the two devices during the generation of the two distant outcomes (see Fig.2).

Looking at Eq. (3), condition (C1) implies, for instance, that the measured quantum state is independent of x and y . Condition (C2) imposes the tensor product and that the measurements on one device do not depend on the input on the other. To guarantee these conditions the user needs to make physical assumptions on the devices (albeit not on their internal working).

3 Protocols

We now provide a unified description of most of the protocols for DIQRNG proposed so far. In general, these protocols involve $n \geq 2$ devices, each having an input x_i and an output a_i for $i = 1, \dots, n$. Condition (C1) imposes that the inputs (x_1, \dots, x_n) must be selected in a way that is uncorrelated to the devices. A standard, yet not the only, way of satisfying this condition is by choosing the inputs using a random *seed*, which has to meet some “independence” requirements depending on the protocol (see below).

¹In what follows some results are illustrated by means of the CHSH inequality, which is the simplest Bell inequality. However, the main ideas and concepts discussed throughout this work apply to any Bell inequality.

DIQRNG PROTOCOL

1. **Data collection.** Repeat N_r times steps (a), (b), (c):
 - (a) A source of n -partite entangled states sends a particle to each of the n devices.
 - (b) Part of the seed is processed to generate a sample from the prior distribution $P(x_1, \dots, x_n)$ of the inputs applied to each device. This distribution can be optimized before the protocol to suit the statistics of the devices.
 - (c) Measurement x_i is performed on device i generating outcome a_i . The inputs and outputs of the devices $(a_1, \dots, a_n, x_1, \dots, x_n)$ are stored.
2. **Non-locality estimation.** Calculate the relative frequency of every combination of inputs/outputs $P_{\text{freq}}(a_1, \dots, a_n | x_1, \dots, x_n)$ using the raw data collected in the N_r rounds. From this data, estimate the non-locality of the observed correlations and determine the length N_k of the final random bit string. The larger the amount of non-locality, the longer N_k . If the observed non-locality is insufficient then the protocol is aborted, $N_k = 0$.
3. **Classical post-processing.** Generate the final N_k -bit string using the raw data collected in the N_r rounds plus additional part of the seed. This process is often made with a so-called randomness “extractor” [17, 18].

A series of parameters that are relevant for the design of DIQRNG protocols are:

Efficiency. Trade-off between the amount of randomness generated and the resources consumed by the DIQRNG protocol. Examples of these resources are the amount of random bits of the seed N_s or the number of uses of the devices N_r .

Quality of the seed. The random seed may not be perfect. For instance, the seed may not be necessarily uniformly distributed, or display correlations with the devices or the adversary. Another possibility is to assume the existence of a good and free source of public randomness, such as the broadcast by NIST’s Randomness Beacon [19]. In this case, the protocol generates private randomness from public randomness.

Robustness. Tolerance of the protocol to noise and imperfections. This allows for using realistic noisy apparatuses. A protocol is robust if it works ($N_k > 0$) for violations above some threshold, which does not need to coincide with the local bound.

Number of devices used in the protocol. The minimum is $n = 2$.

Composability. Protocols should be such that, if the adversary learns some information about the N_k final random bits, she should be able to deduce essentially no additional information [20].

Physical assumptions. Many protocols assume that all the devices and the adversary are constrained by the laws of quantum mechanics. As mentioned, it is possible to relax this requirement and assume only the validity of the no-signalling principle. Even when the security of the protocol does not rely on the validity of quantum mechanics, quantum technology is still needed to generate Bell-violating correlations.

A series of works have focused on efficiency, trying to optimize the trade-off between initial and final randomness. The corresponding protocols are known as randomness expansion protocols [14, 15, 21, 22, 23, 24, 25, 26, 27]. Remarkably, it has been proven that an unbounded amount of randomness ($N_k \rightarrow \infty$) can be generated from a finite seed [23, 25].

Other works [23, 25, 28, 29, 30, 31, 32, 33] have focused on the second point and study how arbitrarily good randomness can be generated in Bell setups using sources of imperfect randomness. These protocols are often known as *randomness amplification* protocols [28]. A commonly used model for the imperfect seed (s_1, s_2, \dots) is a Santha-Vazirani source [34], which is characterized by a parameter $\epsilon \in (0, 1/2)$ such that

$$\epsilon \leq P(s_i | s_1, s_2, \dots, s_{i-1}, \text{devices, Eve}) \leq 1 - \epsilon, \quad (5)$$

for all i . Thus, the larger the value of ϵ , the higher the randomness of the bits. Other models for the seed, more general than the Santha-Vazirani source, have also been considered, such as min-entropy sources [25, 31]. In the case of Santha-Vazirani (5), the performance of randomness amplification protocols is measured by comparing the parameter ϵ_i of the initial source with the final ϵ_f of the generated bits. Full randomness amplification is attained when a source with $\epsilon_i \rightarrow 0$ is mapped to one with $\epsilon_f \rightarrow 1/2$ [29]. From a fundamental point of view, the existence of protocols attaining full randomness amplification is important; we come back to this point below. However, from a practical point of view, while allowing for non-perfect seed is a good addition to the security of a protocol, in most applications one can assume that the seed is uncorrelated to the adversary and devices, and the expansion rate is a more practical figure of merit. Randomness expansion and amplification protocols are sides of the general problem, which is the generation of device-independent private randomness under the minimal set of assumptions and with minimal resources (see Table 1).

	n	$N_k(N_s)$	N_k/N_r	seed quality	seed privacy	QM
Chung...[25]	large	∞	0	$\epsilon > 0$	no	yes
Miller...[24]	2	exp	> 0	$\epsilon = 1/2$	yes	yes
Ramanathan...[32]	2	small	0	$\epsilon > 0$	yes	no
IDEAL	2	∞	> 0	$\epsilon > 0$	no	no

Table 1: **State of the art in DIQRNG protocols.** Properties of the best known protocols, which are robust and composable. They are also immune to attacks exploiting memory effects on the devices, as in the memory loophole introduced in the context of Bell inequality violations [91]. The parameters are, from left to right: number of devices n , amount of expansion of the initial seed, efficiency rate, seed quality ϵ in terms of Eq. (5), whether the seed can be published without compromising security, and whether the security of the protocol relies on the validity of quantum mechanics (QM). The last row contains the ideal optimal value for each parameter.

Before concluding, it is worth recalling that Bell-certified randomness is also a resource for device-independent quantum key distribution [11, 13, 27, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46]. The goal here, however, is not only to generate randomness, but to establish a secret key between two distant users using a Bell violation observed between their devices. In particular, and in contrast to the case of randomness generation, the devices are held in two separate locations and the channel between them is accessible to the eavesdropper.

4 Implementations

The implementation of the previous DIQRNG protocols requires the observation of a Bell inequality violation. For that, it is needed to prepare an entangled state of $n \geq 2$ particles, which are distributed to n devices where they are subjected to local measurements. Assuming the validity of quantum physics, the experimental setup should guarantee that conditions (C1) and (C2) are met so that the observed statistics is correctly described by (3).

An important experimental challenge for the observation of Bell inequality violations is that a high detection efficiency, approximately $\gtrsim 70\%$, is required to close the detection loophole [47]. The loophole says that for low enough detection efficiencies, the statistics of a Bell experiment can always be described by an EPR model, which is deterministic, and thus no randomness certification is possible [48, 49]. Closing the detection loophole is demanding because it concerns any losses in the setup. But it is a loophole that can be completely, and actually has been closed [50, 51, 52, 53, 54, 55, 56, 57]. This is because the loophole does not put into question the validity of description (3), but simply demands a high enough detection efficiency.

Contrary to the detection loophole, the locality [58], collapse-locality [59] and free-will [60] loopholes do put into question the validity of Eq.(3). Because of this, they can never be strictly closed, but their plausibility can be enforced by making physically motivated assumptions on the experimental arrangement. The locality loophole affects condition (C2), that is, whether the measurements in either device do not depend on what happens on the other device. The standard solution adopted is to invoke Einstein’s relativity and arrange the measurements so that they define space-like separated events and no communication can take place between the two devices. This is a very satisfactory solution but also demanding. In our view, there are relevant scenarios in which it is also possible to assume the validity of (C2) without space-like separated measurements. For example, some mild level of trust may be put on the provider so that it is safe to assume that the devices do not signal to each other when producing the outputs given the inputs. Or some level of shielding, always essential for any cryptographic use of the generated numbers, may be assumed, which can in turn be used to avoid any unwanted communication among the devices.

Moreover, the space-like arrangement usually adopted to “close” the locality loophole also assumes that there is a precise knowledge on when the local measurements start and end, that is, when the inputs x, y are defined and the outputs a, b produced. This issue connects with the free-will and collapse-locality loopholes, which also put into question condition (C1). If there is no timing information about when the inputs are generated, this information could for instance exist before the entangled state is produced, i.e., the state in (3) could depend on x and y . A proposed theoretical solution is that the inputs are generated by human beings, hence the term “free will”. The usual and more practical approach to close the loophole is to use a standard QRNG [60]. It is however questionable whether (and if so why) a QRNG is preferable over other processes of classical origin [61]. Similar considerations apply to the timing of the outputs, as in the collapse-locality loophole: one needs to define when the classical results are actually produced to guarantee that the measurements define space-like separated events.

Taking into account all these points and the technological state of the art, there appear two setups in which to implement DIQRNG protocols: entangled particles in separate locations and entangled photons. In the first case, a Bell test is performed between two distant massive particles, such as nitrogen-vacancy (NV) centres [55], or ions in two traps [51, 52] that have been entangled through entanglement swapping on two photon-particle entangled pairs [62, 63]. The advantage of this setup is that massive particles can be measured with almost perfect efficiency, thus, closing the detection loophole. In fact, a first proof-of-principle demonstration of DIQRNG, reporting a generation rate of 42 random bits after approximately one month of

measurements, was performed using two entangled ions in two traps at 1 meter distance [15]. This rate is valid under the assumption that the experimental setup was not operating in a malicious way [21]. While challenging, setups with entangled distant particles also allow arranging the measurements so that one can reasonably assume that both the detection and locality loopholes are closed. This was achieved in [55] and subsequently in [64]. However, these experiments do not report any analysis of random-number generation.

The second solution consists of performing polarisation measurements on two entangled photons. Historically, one of the main challenges in these setups was that photon-detection efficiencies were too low to close the detection loophole. However, advances on photo-detectors have allowed closing it [53, 54]. The first experiment only focused on the Bell violation, but the second reported a random-number generation rate of 0.4 bits/s. More recently, the locality loophole has also been closed in photonic experiments [56, 57], but again none of these experiments were analysed for DIQRNG.

5 Other methods for randomness generation

Since meeting conditions (C1) and (C2) in an experiment is challenging, alternative proposals for certified quantum randomness generation have been proposed. The idea is to keep part of the device-independent spirit and make only some mild assumptions about the setup, yet without any detailed modelling of the devices. Randomness certification comes from a purely quantum effect with no classical analogue, under the mentioned assumptions. Standard QRNG do not fit into this category, as they require modelling and certify randomness using statistical tests that are also satisfied by classical RNG.

A series of works have explored information protocols under a dimensional constraint [65, 66], a scenario known as semi-device-independent. The setup is different from a Bell test and consists of a preparing device that prepares a system in different quantum states and a measuring device that performs measurements on it. It is then assumed that the states prepared by the first device and measured by the second belong to a Hilbert space of dimension not larger than d . This is the extra assumption that goes beyond the fully DI paradigm. Randomness certification is then obtained via the violation of the so-called dimension witnesses [67]. One of the practical advantages of this approach is that it does not require the generation of entanglement. The required detection efficiencies are smaller, but still demanding [49]. A solution to this problem was suggested in [68], where it was shown that schemes in which one assumes that the preparation and measuring device share no correlations, and that devices do not display memory effects, certify the presence of randomness for any value of the detection efficiency. An proof-of-principle experimental demonstration of this proposal was also performed in [69], although a security proof for these schemes without assumptions on memory effects is lacking.

A second proposal considers an asymmetric scenario in which some of the devices are fully trusted. For instance, one may trust preparing but not the measuring devices. Asymmetric scenarios are often considered in the context of steering [70]. This is a concept defined in the same setup as non-locality, in which two parties perform measurements on two distant quantum particles, but now one of the devices is fully trusted. The detection of steering provides a quantum certification sufficient to guarantee the presence of randomness [71]. Steering has been experimentally demonstrated with the detection and locality loopholes closed [72, 73, 74], but the detection efficiencies needed for randomness expansion still pose an important challenge [49]. Security proofs are in a preliminary stage also in the case of steering. A general security proof was provided in [75], but it requires a very low level of noise.

6 Fundamental questions on randomness

The results connecting randomness and non-locality are relevant not only for applications of quantum technologies, but also for our understanding of physics. Protocols attaining full randomness amplification against non-signalling eavesdroppers represent the strongest form of certification using quantum physics of the existence of random events in nature. It is impossible to certify randomness from scratch. Under only the assumption of no-signalling, the violation of Bell inequalities certifies the presence of randomness, but requires some initial randomness. Full randomness amplification protocols [23, 25, 29, 30, 31, 32, 33] are not able to completely break this circularity, but relax it as much as possible.

Historically, the whole discussion on EPR models and Bell inequalities was motivated by the search for a “complete” alternative to quantum theory, in the sense that measurement outcomes could have a deterministic description within the alternative theory. The violation of Bell inequalities implies that quantum predictions can not be completed into a deterministic theory without violating the no-signalling principle. In recent years, stronger proofs of the “uncompleteness” of quantum theory have appeared [11, 13, 76, 77, 78]. These works show that a no-signalling model, possibly non-deterministic, having higher predictive power than quantum theory does not exist. Full randomness amplification protocols against no-signalling eavesdroppers can also be seen as proofs for the uncompleteness of quantum theory. Along a similar motivation, the study of randomness is also relevant when comparing quantum theory with more general theories respecting the no-signalling principle [9, 79]. It has been shown that theories leading to general non-signalling correlations do not allow for maximal randomness certification, while quantum theory does [80].

Finally, a series of works have shown that the relation between entanglement, non-locality and randomness is subtler than expected. For instance, states with arbitrarily small amounts of entanglement (and non-locality) allow for maximal randomness certification [81]. Recent progress in this direction also shows that the use of more complex measurements, such as non-projective [82] or sequences of measurements [83], provides further advantages for randomness certification. Despite all these results, a complete understanding of the relation between entanglement, non-locality and randomness is still missing.

7 Outlook

DIQRNG protocols represent a change of paradigm for randomness that solve fundamental and practical drawbacks of standard RNG schemes. On the theory side, the existing security proofs show the validity of the approach. Further theoretical studies are however needed to understand how to relax the requirements for DIQRNG. The ultimate goal would be to design a robust and composable secure protocol attaining an infinite randomness expansion rate using initial sources of arbitrarily weak public randomness with only two devices, and assuming only the validity of the no-signalling principle (see Table 1). While this ambitious goal may be unreachable, there is still a lot of room for improvement on the conditions needed for DI randomness generation.

On the implementation side, it is expected that new DIQRNG experiments using the setups explained above will be reported in the coming years with a constantly improved generation rate. Looking ahead, integrated photonic circuits and solid-state setups appear as other platforms in which to run the previous protocols. To our knowledge, however, no Bell experiment has been reported on integrated photonic circuits. Bell non-local correlations in solid-state devices have been reported for two [84, 85] and three systems [86, 87]. These technologies could be more promising in terms of miniaturisation and, thus, the possible construction of commercial DIQRNG devices. Miniaturisation however comes at a price, as the possible validity of condition

(C2) becomes less clear, even if one is ready to accept that measurements don't need to be space-like separated. Theoretical solutions to take into account cross-talk effects have been proposed in [88]. In fact, the analysis of DIQRNG implementations opens new theoretical questions, such as: (i) which are the detection efficiencies needed for randomness expansion [49]? (ii) which Bell setups are more robust against noise, or detection inefficiencies [89]? (iii) how to deal with detection inefficiencies [90]?

This is nothing but the natural evolution of this research line, where theory and implementation are joining efforts to design more robust and feasible schemes. RNG with unprecedented standards of quality and security seem within reach using quantum technologies.

Acknowledgments. We thank Stefano Pironio, Valerio Scarani, Rotem Arnon Friedman and Andreas Wallraff for discussions. AA acknowledges support from the ERC CoG QITBOX, the AXA Chair in Quantum Information Science, Spanish MINECO (FOQUS FIS2013-46768-P and SEV-2015-0522), Fundaci3n Cellex, the Generalitat de Catalunya (SGR 875) and The John Templeton Foundation. LM is supported by EPSRC.

References

- [1] Rukhin, A. *et al.* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *NIST Special Publication 800-22rev1a*, National Institute of Standards and Technology (2010); available at <http://csrc.nist.gov/groups/ST/toolkit/rng/index.html>.
- [2] Von Neumann, J. Various techniques used in connection with random digits. *National Bureau of Standards Applied Mathematics Series 12*, 36-38 (1951).
- [3] Markowsky, G. The sad history of random bits. *Journal of Cyber Security and Mobility 3*, 1-24 (2014).
- [4] Bell, J. S. On the Einstein Podolsky Rosen Paradox. *Physics 1*(3), 195-200 (1964).
- [5] Einstein, A., Podolsky, B. & Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **47**, 777-780 (1935).
- [6] Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23** 880-884 (1969).
- [7] Khalfin, L. A. & Tsirelson, B. S. in *Symposium on the Foundations of Modern Physics* (eds Lahti, P. & Mittelstaedt, P.) 441-460 (World Scientific Publishers, Singapore,1985).
- [8] Tsirelson, B.S. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement 8*(4), 329-345 (1993).
- [9] Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24**(3) 379-385 (1994).
- [10] Valentini, A. Signal-Locality in Hidden-Variables Theories. *Phys. Lett. A* **297**, 273-278 (2002).
- [11] Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95** 010503 (2005).

- [12] Masanes, L., Acín & Gisin, N. General properties of Nonsignaling Theories. *Phys. Rev. A.* **73**, 012112 (2006).
- [13] Barrett, J., Kent, A. & Pironio, S., Maximally Non-Local and Monogamous Quantum Correlations. *Phys. Rev. Lett.* **97**, 170409 (2006).
- [14] Colbeck, R. Quantum And Relativistic Protocols For Secure Multi-Party Computation. PhD Thesis, University of Cambridge (2006); Preprint at <http://arxiv.org/abs/0911.3814>.
- [15] Pironio, S. *et al.*, Random Numbers Certified by Bell's Theorem. *Nature* **464**, 1021-1024 (2010).
- [16] Hall, M. J. W. Complementary contributions of indeterminism and signalling to quantum correlations. *Phys. Rev. A* **82**, 062117 (2010).
- [17] Trevisan, L. Extractors and pseudorandom generators. *J. ACM*, 860-879 (2001).
- [18] Nisan N. & Ta-Shma A. Extracting randomness: A survey and new constructions. *J. Comp. Syst. Sci.* **58**, 148-173 (1999).
- [19] National Institute of Standard and Technologies, Randomness beacon project, http://www.nist.gov/itl/csd/ct/nist_beacon.cfm.
- [20] Canetti, R. Universally Composable Security: A New Paradigm for Cryptographic Protocols. *Proc. 42nd IEEE Symposium on Foundations of Computer Science (FOCS)*, 136 (2001).
- [21] Colbeck, R. & Kent, A. Private Randomness Expansion With Untrusted Devices, *J. Phys. A: Math. Th.* **44**(9), 095305 (2011).
- [22] Vazirani, U. V. & Vidick, T. Certifiable Quantum Dice. *Phil. Trans. R. Soc. A*, **370**, 3432-3448 (2012).
- [23] Coudron, M. & Yuen, H. Infinite Randomness Expansion and Amplification with a Constant Number of Devices. Preprint at <http://arxiv.org/abs/1310.6755>.
- [24] Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. Preprint at <http://arxiv.org/abs/1402.0489>.
- [25] Chung, K. M., Shi, Y. & Wu, X. Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions. Preprint at <http://arxiv.org/abs/1402.4797>.
- [26] Miller, C. A. & Shi, Y. Universal security for randomness expansion from the spot-checking protocol. Preprint at <http://arxiv.org/abs/1411.6608>.
- [27] Arnon-Friedman, R. Renner, R. & Vidick, T. Simple and tight device-independent security proofs. Preprint at <http://arxiv.org/abs/1607.01797>.
- [28] Colbeck, R. & Renner, R. Free randomness can be amplified. *Nature Phys.* **8**(6), 450-454 (2012).
- [29] Gallego, R. *et al.* Full randomness from arbitrarily deterministic events. *Nature Comm.* **4**, 2654 (2013).
- [30] Brandão, F.G.S.L., *et al.* Robust Device-Independent Randomness Amplification with Few Devices. *Nature Comm.* **7**, 11345 (2016).

- [31] Bouda, J., Pawłowski, M., Pivoluska, M. & Plesch, M. Device-independent randomness extraction for arbitrarily weak min-entropy source. *Phys. Rev. A* **90**, 032313 (2014).
- [32] Ramanathan R. *et al.* Randomness Amplification against no-signaling adversaries using two devices Preprint at <http://arxiv.org/abs/1504.06313>.
- [33] Wojewódka, H. *et al.* Amplifying the randomness of weak sources correlated with devices. Preprint at <http://arxiv.org/abs/1601.06455>.
- [34] Santha, M. & Vazirani, U. Generating quasi-random sequences from slightly-random sources. *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS-84)*, 434-440 (1984).
- [35] Mayers, D. & Yao, A. Self testing quantum apparatus. *Quant. Inform. Comput.* **4** 273-286 (2004).
- [36] Acín, A., Gisin, N. & Masanes, L. From Bell's Theorem to Secure Quantum Key Distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
- [37] Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
- [38] Masanes, L. Universally-composable privacy amplification from causality constraints. *Phys. Rev. Lett.* **102**, 140501 (2009).
- [39] Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).
- [40] Hänggi, E. & Renner, R. Device-independent quantum key distribution with commuting measurements. Preprint at <http://arxiv.org/abs/1009.1833>.
- [41] Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Comm.* **2**, 238 (2011).
- [42] Masanes, L. , Renner, R., Christandl, M., Winter, A. & Barrett, J. Full security of key distribution from no-signaling constraints. *IEEE Trans. Inf. Theory* **60**, 4973-4986 (2014).
- [43] Barrett, J., Colbeck, R., & Kent, A. Unconditionally secure device-independent quantum key distribution with only two devices. *Phys. Rev. A* **86**, 062326 (2012).
- [44] Reichardt, B., Unger, F. & Vazirani U. Classical command od quantum systems. *Nature* **496**, 456-460 (2013).
- [45] Barrett, J., Colbeck, R. & Kent, A. Memory Attacks on Device-Independent Quantum Cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).
- [46] Vazirani, U. & Vidick, T. Fully device independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
- [47] Pearle, P. Hidden-Variable Example Based upon Data Rejection. *Phys. Rev. D* **2**, 1418-1425 (1970).
- [48] Massar, S & Pironio, S. Violation of local realism vs detection efficiency. *Phys. Rev. A* **68**, 062109 (2003).

- [49] Acín, A., Cavalcanti, D., Passaro, E., Pironio, S. & Skrzypczyk, P. Detection attacks on cryptographic protocols and bound randomness. *Phys. Rev. A* **93**, 012319 (2016).
- [50] Rowe M. A. *et al.* Experimental violation of a Bell’s inequality with efficient detection. *Nature* **409**, 791-794 (2001).
- [51] Matsukevich, D. N., Maunz, P., Moehring, D. L., Olmschenk, S. & Monroe, C. Bell inequality violation with two remote atomic qubits. *Phys. Rev. Lett.* **100**, 150404 (2008).
- [52] Hofmann J. *et al.* Heralded entanglement between widely separated atoms. *Science* **337**, 72-75 (2012).
- [53] Giustina M. *et al.* Bell violation with entangled photons, free of the fair-sampling assumption. *Nature* **497**, 227-230 (2013).
- [54] Christensen, B. G. *et al.*, Detection-Loophole-Free Test of Quantum Nonlocality, and Applications *Phys. Rev. Lett.* **111**, 130406 (2013).
- [55] Hensen, B. *et al.*, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, **526**, 682-686 (2015).
- [56] Giustina, M. *et al.* Significant-loophole-free test of Bell’s theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
- [57] Shalm, L. K. *et al.* A strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
- [58] Aspect, A. Proposed experiment to test separable hidden-variable theories. *Phys. Lett. A* **54**, 117-118 (1975).
- [59] Kent, A. Causal Quantum Theory and the Collapse Locality Loophole. *Phys. Rev. A* **72**, 012107 (2005).
- [60] Scheidl, T. *et al.* Violation of local realism with freedom of choice, *PNAS* **107**(46), 19708-19713 (2010).
- [61] Pironio, S. Random ‘choices’ and the locality loophole. Preprint at <http://arxiv.org/abs/1510.00248>.
- [62] Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A.K. “Event-ready-detectors” Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287-4290 (1993).
- [63] Simon, C. & Irvine, W. T. M. Robust long-distance entanglement and a loophole-free Bell test with ions and photons. *Phys. Rev. Lett.* **91**, 110405 (2003) .
- [64] Hensen, B. *et al.* Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis. Preprint at <http://arxiv.org/abs/1603.05705>.
- [65] Pawłowski, M. & Brunner, N. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A* **84**, 010302(R) (2011).
- [66] Li, H.-W., Pawłowski, M., Yin, Z.-Q., Guo, G.-C. & Han, Z.-F. Semi-device independent random number expansion protocol with n to 1 quantum random access codes. *Phys. Rev. A* **85**, 052308 (2012).

- [67] Gallego, R., Brunner, N., Hadley, C. & Acín, A. Device-independent tests of classical and quantum dimensions. *Phys.Rev.Lett.* **105**, 230501 (2010).
- [68] Bowles, J., Quintino, M. T. & Brunner, N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Phys. Rev. Lett.* **112**, 140407 (2014).
- [69] Lunghi T. *et al.* A self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).
- [70] Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, Entanglement, Nonlocality, and the EPR Paradox. *Phys. Rev. Lett.* **98**, 140402 (2007).
- [71] Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided Device-Independent Quantum Key Distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A* **85**, 010301(R) (2012).
- [72] Smith, D. H. *et al.* Conclusive quantum steering with superconducting transition edge sensors. *Nature Comm.* **3**, 625 (2012).
- [73] Bennet, A. J. *et al.* Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole. *Phys. Rev. X* **2**, 031003 (2012).
- [74] Wittmann, B. *et al.* Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering. *New J. Phys.* **14**, 053030 (2012).
- [75] Tomamichel, M., Fehr, S., Kaniewski, J. & S. Wehner. A Monogamy-of-Entanglement Game With Applications to Device-Independent Quantum Cryptography. *New J. Phys.* **15**, 103002 (2013).
- [76] Colbeck R. & Renner, R. No extension of quantum theory can have improved predictive power. *Nature Comm.* **2**, 411 (2011).
- [77] Colbeck R. & Renner, R. Is a system's wave function in one-to-one correspondence with its elements of reality?. *Phys. Rev. Lett.* **108**, 150402 (2012).
- [78] Dhara, C. , de la Torre, G. & Acín, A. Can observed randomness be certified to be fully intrinsic?. *Phys. Rev. Lett.* **112**, 100402 (2014).
- [79] Barrett, J. *et al.* Non-local correlations as an information theoretic resource. *Phys. Rev. A* **71**, 022101 (2005).
- [80] de la Torre, G. , Hoban, M. J. , Dhara, C. , Prettico, G. & Acín A. Maximally nonlocal theories cannot be maximally random. *Phys. Rev. Lett.* **114**, 160502 (2015)
- [81] Acín, A., Massar, S. & Pironio, S. Randomness versus Non Locality and Entanglement. *Phys. Rev. Lett.* **108**, 100402 (2012).
- [82] Acín, A. , Pironio, S. , Vértesi, T. & Wittek, P. Optimal randomness certification from one entangled bit. *Phys. Rev. A* **93**, 040102 (2016).
- [83] Curchod, F. J. *et al.* Unbounded randomness certification using sequences of measurements. Preprint at <http://arxiv.org/abs/1510.03394>.

- [84] Ansmann, M. *et al.* Violation of Bell's inequality in Josephson phase qubits. *Nature* **461**, 504-507 (2009).
- [85] Dehollain, J. P. *et al.* Bell's inequality violation with spins in silicon. *Nature Nanotechnology* **11**, 242-246 (2016).
- [86] Neeley, M. *et al.* Generation of three-qubit entangled states using superconducting phase qubits. *Nature* **467**, 570-573 (2010).
- [87] DiCarlo, L. Preparation and measurement of three-qubit entanglement in a superconducting circuit. *Nature* **467**, 574-578 (2010).
- [88] Silman, J., Pironio, S. & Massar, S. Device-Independent Randomness Generation in the Presence of Weak Cross-Talk. *Phys. Rev. Lett.* **110**, 100504 (2013).
- [89] Máttar, A., Skrzypczyk, P., Brask, J. B., Cavalcanti, D. & Acín, A. Optimal randomness generation from optical Bell experiments. *New J. Phys.* **17**, 022003 (2015).
- [90] Thinh, L. P., de la Torre, G., Bancal, J.-D., Pironio, S. & Scarani, V. Randomness in post-selected events. *New J. Phys.* **18**, 035007 (2016).
- [91] Barrett, B. Collins, D., Hardy, L., Kent A. & Popescu, S. Quantum nonlocality, Bell inequalities and the memory loophole. *Phys. Rev. A* **66**, 042111 (2002).
- [92] Navascués, M., Pironio, S. & Acín, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98**, 010401 (2007).
- [93] Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10**, 073013 (2008).
- [94] Nieto-Silleras, O., Pironio, S. & Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. *New J. Phys.* **16**, 013035 (2014).

Competing financial interests

The authors declare no competing financial interests.

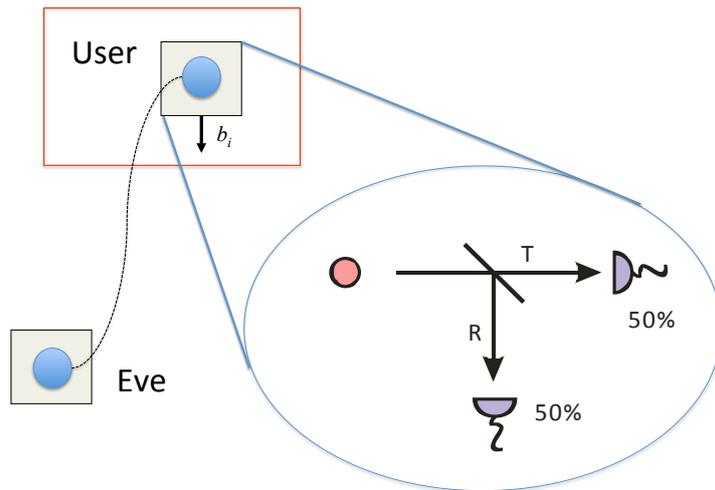


Figure 1: **Schemes for randomness generation.** The user, in his secure location, has access to a device that generates bits, b_i . The user wants to make sure that the value of these bits cannot be predicted by any observer outside his lab. The way to model this is by an external super-observer who has access to all that is beyond the user's location, represented by another device that may be correlated to the user's device. It is useful to interpret the external observer as an adversary or eavesdropper, Eve, who wants to predict the generated bits (for instance to break any possible use for cryptographic applications). The generated bits should be unpredictable to Eve, even after measuring her device. For standard QRNG, the random character of the outputs follows from assumptions on the inner working of the user's device. The figure displays a scheme based on a single photon (red ball) impinging a beam-splitter with transmission coefficient equal to $1/2$. Two single-photon detectors placed at the two arms of the interferometer measure the path taken by the photon. According to quantum physics, this process is probabilistic and the probability that a given detector clicks is equal to the transmission coefficient of the beam-splitter, assumed to be $1/2$.

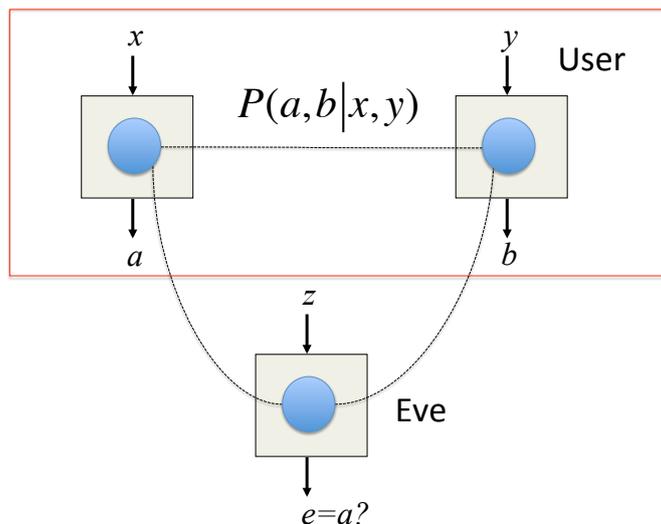


Figure 2: **Structure of DIQRNG protocols.** In a general protocol for DIQRNG the user has access to $n \geq 2$ correlated devices. The figure shows the the simplest case of two devices, which generate classical outputs a and b , after applying the inputs x and y (the generalisation to more devices is straightforward). The inputs x and y can be understood as the labels of the measurement performed on each device and the outputs as the obtained results. The external (eavesdropping) observer, Eve, may have a system correlated with the user's devices. The randomness of one of the outputs, say a , can be quantified by the optimal probability P_{guess} that Eve guesses it correctly, $e = a$, after performing a measurement z on her system [14, 15, 81]. In the case of quantum eavesdroppers, the guessing probability is optimized over all quantum preparations, including the tripartite state and measurements, compatible with the correlations observed by the user [15, 92, 93, 94]. One can relax the assumption on the validity of quantum mechanics, and consider eavesdroppers who can prepare any tripartite correlations compatible with the no-signaling principle, even beyond quantum physics [15, 94].

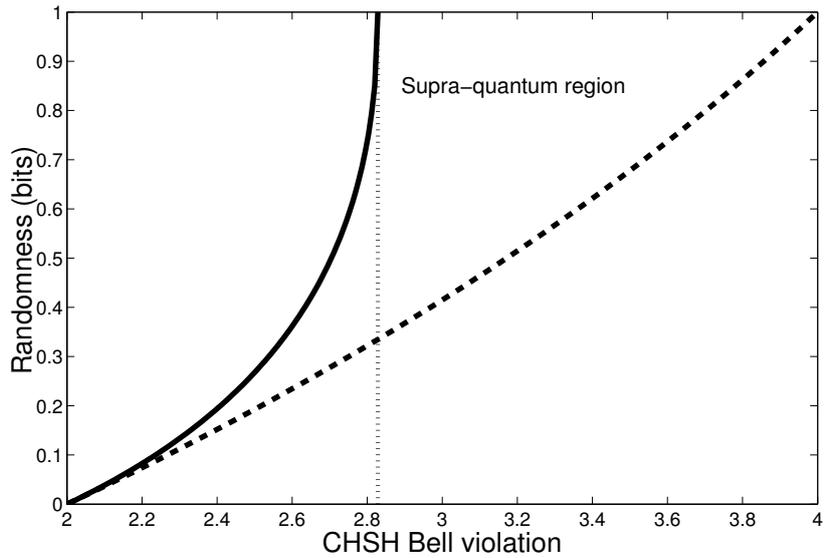


Figure 3: **Randomness for the CHSH Bell inequality.** Optimal guessing probabilities for one of the outputs, shown in bits, $-\log_2 P_{\text{guess}}$, as a function of the CHSH inequality violation observed by the user. These curves are computed using the techniques in [15, 81]. The solid line refers to a quantum eavesdropper, while the dashed line is for a non-signalling eavesdropper. The quantum violation of the CHSH inequality is upper bounded by $2\sqrt{2}$, while it is possible to get larger supra-quantum violations without breaking the no-signalling principle. At the local bound, CHSH violation equals 2, no randomness can be certified, while some randomness appears for any non-zero violation. In both cases, a perfect random bit is certified by the corresponding maximal Bell violation.